Enterprise Design Patterns: Configuration Management

- **Design Pattern Scope:** This Enterprise Design Pattern provides a vendor-agnostic process framework, based on IT Infrastructure Library (ITIL) best practices and enterprise capabilities that VA will use to implement enterprise-wide IT service Configuration Management. This framework includes standardized processes and toolsets to manage VA's IT service configuration items, leading to reduced security vulnerabilities and enhanced customer support across all Lines of Business.

- **Current State:** Recent VA Office of the Inspector General (OIG), Federal Information Security Management Act (FISMA) and Federal Identity, Credential, and Access Management (FICAM) identified material weaknesses stemming from a fragmented approach to IT asset management. These assets include all of the CIs that make up IT services. A consistent approach and toolset for managing these CIs ensures that the entire infrastructure satisfies functional and non-functional requirements, which includes all Service Level Agreements (SLAs). As a result, all infrastructure hosting environments have unified control over potential vulnerabilities and unexpected configuration changes that inhibit VA's ability to meet customer expectations.

- **Design Pattern Solution:** An IT infrastructure spanning across numerous hosting environments requires a consistent approach to managing its service assets and configuration items (CI). A common set of IT service management (ITSM) tools and processes is required to ensure flexibility to changing business needs and adherence to enterprise security policies. The document sections establish a framework for enterprise-wide Configuration Management (CM) capabilities. The framework addresses the following challenges:
    - ITSM Configuration Management (CM) capabilities are not fully utilized and are dispersed geographically.
    - Lack of standardized processes for IT service assets and CM.
    - An enterprise-level Configuration Management System (CMS) has not been identified.
    - Ownership and resources to manage an enterprise CMS have not been identified.

  VA's near-term approach to establishing and deploying an enterprise configuration management capability includes the following activities:
    - Establishment of a standard CM methodology (ongoing)
    - Evaluation of current CM toolset (ongoing)
    - Selection of an enterprise-wide CM toolset (planned)
    - National implementation of standard CM methodology and toolset (planned)

  Deploying an enterprise-wide CM capability will enable a logical view of all CIs across the enterprise. This capability will support the evaluation of IT assets against the Technical Reference Model (TRM) to ensure approved products are used in the enterprise.

  The enterprise-wide CM approach aligns to the CM process already published in ProPath and aligned to NIST SP 800-128.
  The following figure shows the high-level CM process based on NIST guidance.

Planning → Identifying and Implementing Configurations → Controlling Configuration Changes → Monitoring